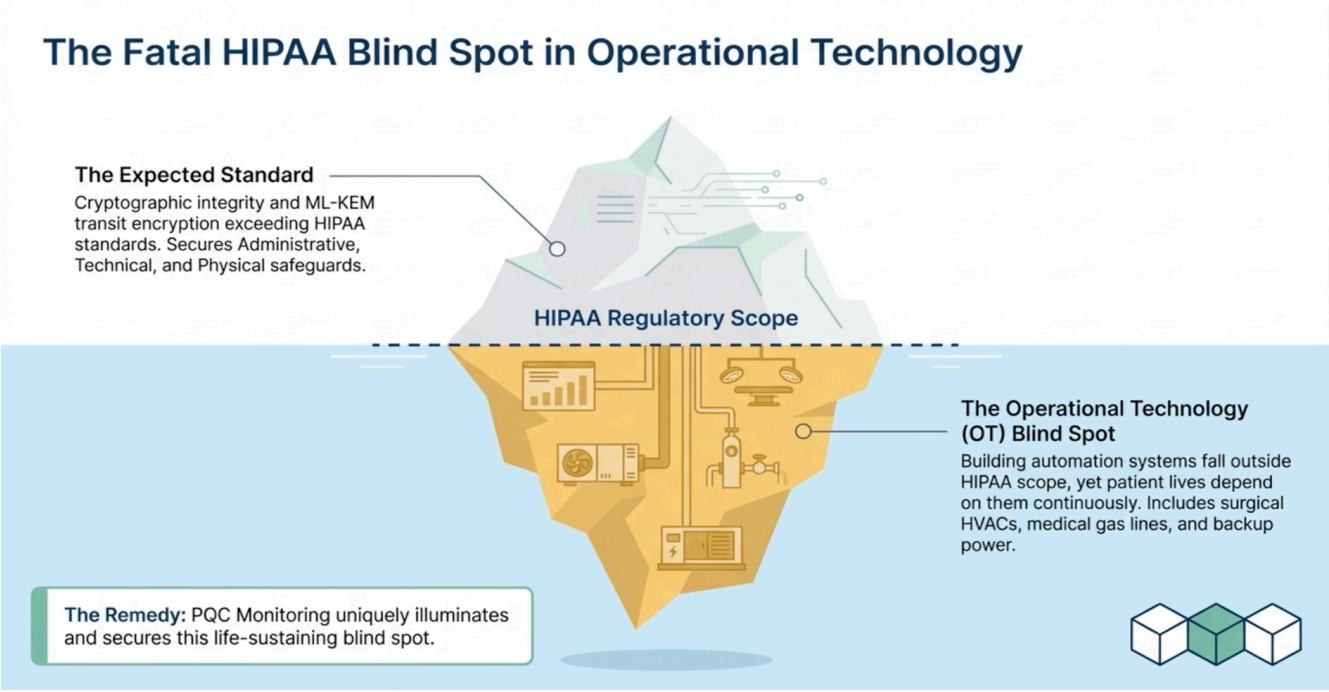
RHT Comprehensive Compliance Solution

Ensuring Federal & 50-State Regulatory Compliance +
Post-Quantum Cryptography with PQC+ Software Platform



PQC+ is the future of secure, compliant healthcare operations, providing a **Unified RHT Compliance + Post-Quantum Security Framework that seamlessly integrates federal and 50-state regulatory compliance with US military-grade Operational Technology (OT) and the only PQC that can be fully installed in 60 to 90 days.** By ensuring your compliance and safeguarding cybersecurity your continued eligibility for RHT payments is assured.

Our Unique Value Proposition

1. **Unmatched Compliance Scope:** Our robust framework minimizes unnecessary audits and drives significant savings by covering and optimizing 10 domains, over 60 control requirements, 8 sensitive data categories, 5 AI consent use cases, 8 building automation system types, and 9 proxy authority types.
2. **Universal MDM Gateway Security:** Regardless of which Mobile Device Management (MDM) vendor you currently use, our gateway protects your infrastructure against advanced threats, such as the recent "Stryker-like Microsoft MDM" hacker attack incident.
3. **Proprietary AI Compliance Extension:** We offer a universally compatible AI extension built specifically for the industry-standard Anthropic AI's Model Context Protocol (MCP) server. This ensures full federal and 50-state regulatory compliance for all data processed by your organization or business associates.
4. **80% Reduction in ATO Costs and Timelines:** By leveraging the compliance work already completed during our federal FDA Authority To Operate (ATO) authorization, we eliminate redundant control testing and auditing, cutting your state's ATO costs and timelines by 80%.

PQC+ is a 100% software solution with free trialware. Inexpensive, quick and easy to implement. Its unparalleled scope surpasses all other compliance and PQC approaches. We encourage you to first watch the following videos and optionally listen to the tech talk, before reading the tables of this document.

- **Video, Securing the Rural Health Transformation Program**: for gatekeepers and staff
- **Video, RHT Value for CTO/CISO/Attorneys**: for technical personnel
- **Tech Talk**: 21 minute conversation explaining the challenges and our unique PQC+ solution

Software Integrations to Address Requirements & Platform Legend

PQC Monitoring = OT/ICS cybersecurity monitoring platform (behavioral analytics, 340+ protocol parsers, ML ensemble detection) Q-InfoSecur / PQC = Post-quantum cryptographic solution FIPS 140-3, NIST FIPS 203/204/205) TransformativIP Core Modules = TransformativIP patient-centric healthcare data platform (consent management, FHIR interoperability, IP-ACL, SMARTCompliance) ALL = Coverage requires capabilities from TransformativIP Q-InfoSecur /PQC and and Core Modules working together.

Table of Contents

1. CMS Authorization to Operate (ATO - NIST SP 800-53 Rev 5)

Any information system processing, storing, or transmitting CMS/Medicaid data under the RHT program requires a formal ATO following the NIST Risk Management Framework. The CMS Acceptable Risk Safeguards (ARS) tailors NIST 800-53 controls for healthcare. The following maps each relevant control family to the platform(s) providing coverage.

Control Family	Control ID	Requirement Summary	Platform	Software Used to Address Requirement
Access Control	AC-2, AC-3, AC-6	Account management, access enforcement, least privilege for all systems processing Medicaid data	**TransformativIP Core Modules + PQC Monitoring**	**TransformativIP Core Modules: IP-ACL enforces patient-level and role-level access at the data layer; ABAC/RBAC hybrid model. PQC Monitoring: Monitors for unauthorized access attempts, privilege escalation, and access pattern anomalies.**
Access Control	AC-4	Information flow enforcement between security domains	**PQC Monitoring**	**PQC Monitoring: Deep packet inspection monitors all cross-boundary data flows; behavioral baselines detect unauthorized information flow paths between IT and OT segments.**
Access Control	AC-17	Remote access controls and monitoring	**PQC Monitoring**	**PQC Monitoring: Monitors all remote access sessions (VPN, jump server, vendor connections); behavioral analytics detect anomalous remote access patterns; alerts on unauthorized remote access.**
Audit & Accountability	AU-2, AU-3, AU-6, AU-12	Audit event generation, content, review/analysis, and audit generation	**TransformativIP Core Modules + PQC Monitoring**	**TransformativIP Core Modules: Tamper-evident audit trail for every data exchange, consent decision, and access event. PQC Monitoring: Network-level audit logging of all monitored communications; security event correlation and analysis.**
Security Assessment	CA-2, CA-7	Security assessments, continuous monitoring	**PQC Monitoring**	**PQC Monitoring: Provides the continuous monitoring infrastructure (CA-7) required for ongoing ATO authorization. Automated generation of monitoring evidence for security assessment (CA-2).**
Configuration Mgmt	CM-2, CM-3, CM-6, CM-8	Baseline configuration, change control, configuration settings, system component inventory	**PQC Monitoring**	**PQC Monitoring: Passive asset discovery and inventory (CM-8); configuration baseline monitoring and change detection (CM-2, CM-3); configuration deviation alerting (CM-6).**
Identification & Auth	IA-2, IA-5, IA-8	Multi-factor authentication, authenticator management, identification of non-org users	**TransformativIP Core Modules + TransformativIP Q-InfoSecur Module**	**TransformativIP Core Modules: Identity management with ABAC/RBAC for all user and system identities. TransformativIP Q-InfoSecur Module: Hardware-bound post-quantum cryptographic authentication (FIPS 140-3); phishing-resistant MFA resistant to AiTM session token theft.**
Incident Response	IR-4, IR-5, IR-6	Incident handling, monitoring, reporting	**PQC Monitoring**	**PQC Monitoring: Real-time threat detection with MITRE ATT&CK mapping provides incident identification (IR-4); continuous monitoring enables incident trending (IR-5); automated alert generation supports incident reporting (IR-6).**
System & Info Integrity	SI-2, SI-3, SI-4, SI-5	Flaw remediation, malicious code protection, system monitoring, security alerts	**PQC Monitoring**	**PQC Monitoring: SI-4 is the core PQC Monitoring capability — continuous system monitoring with behavioral analytics and anomaly detection. Vulnerability correlation with asset inventory (SI-2). Malicious activity detection without requiring malware signatures (SI-3). CISA/ICS-CERT advisory integration (SI-5).**

System & Comms Protection	SC-7, SC-8, SC-12, SC-13, SC-28	Boundary protection, transmission confidentiality/integrity, crypto key mgmt, crypto protection, data at rest	**TransformativIP Q-InfoSecur Module + PQC Monitoring**	**TransformativIP Q-InfoSecur Module: Post-quantum encryption for data in transit (SC-8) and data at rest (SC-28); FIPS 140-3 validated cryptographic key management (SC-12) and cryptographic protection (SC-13). PQC Monitoring: Network boundary monitoring and enforcement verification (SC-7).**
Risk Assessment	RA-3, RA-5	Risk assessment, vulnerability monitoring and scanning	**PQC Monitoring**	**PQC Monitoring: Passive vulnerability assessment through protocol fingerprinting and version correlation against CVE/NVD/KEV databases (RA-5). Continuous risk scoring informs risk assessment (RA-3).**
Planning	PL-2	System security and privacy plans	**TransformativIP Core Modules + PQC Monitoring**	**Both platforms generate documentation and evidence supporting the System Security and Privacy Plan (SSPP) required for the ATO package.**

To expedite state-level risk acceptance, TransformativIP will supply each State Medicaid Agency CISO with a full, three-part reciprocity documentation package.

(1) Reciprocity Memorandum — A formal request for acceptance of the existing FDA Authorization to Operate as the primary evidentiary basis for state-level ATO, citing the legal basis under NIST SP 800-37 (Risk Management Framework) FISMA reciprocity provisions, HHS inter-agency alignment between FDA and CMS, and the independent FIPS 140-3 cryptographic module validation (CVMP #4482). The memorandum will recommend that the state adopt the FDA authorization package for all controls within the FDA ATO scope and limit local review to state-specific integration points.

(2) FDA ATO Scope Crosswalk — A detailed mapping identifying which controls in the table above were assessed and authorized under the existing FDA ATO (primarily the TransformativIP Q-InfoSecur cryptographic controls and TransformativIP Core Modules identity and consent enforcement modules), which controls are provided by PQC Monitoring and require state-level assessment (continuous monitoring, asset discovery, behavioral detection, incident response), and which controls are shared across platforms and require only a delta review against the FDA baseline. This crosswalk defines the precise scope of the state's independent review, reducing the assessment from a full NIST 800-53 Moderate baseline audit to a targeted evaluation of state-specific integration and net-new capabilities.

(3) Pre-Populated ATO Evidence Package — System Security and Privacy Plan (SSPP) sections, Security Assessment Report (SAR) artifacts from the FDA authorization, FIPS 140-3 validation certificate, and Plan of Action and Milestones (POA&M) templates — pre-populated with platform-level control implementations so that the state's assessment team begins with a substantially complete authorization package rather than starting from scratch.

2. HIPAA Security Rule (45 CFR Parts 160 & 164)

HIPAA Provision	Section	Requirement	Platform	How Addressed
Administrative Safeguards	§164.308(a)(1)	Security management process: risk analysis, risk management, sanction policy, IS activity review	**PQC Monitoring + TransformativIP Core Modules**	**PQC Monitoring: Continuous risk assessment through behavioral monitoring; IS activity review through network-level audit logging. TransformativIP Core Modules: Tamper-evident audit trails for all data access; risk analysis of data sharing patterns.**
Administrative Safeguards	§164.308(a)(5)	Security awareness and training; log-in monitoring; password management	**PQC Monitoring**	**PQC Monitoring: Login monitoring through authentication pattern analysis; detection of brute-force, credential stuffing, and anomalous login behavior.**
Administrative Safeguards	§164.308(a)(6)	Security incident procedures: response and reporting	**PQC Monitoring**	**PQC Monitoring: Automated incident detection, classification, and alerting with MITRE ATT&CK mapping; investigation workflow with evidence preservation.**
Technical Safeguards	§164.312(a)	Access control: unique user identification, emergency access, automatic logoff, encryption	**TransformativIP Core Modules + TransformativIP Q-InfoSecur Module**	**TransformativIP Core Modules: ABAC/RBAC hybrid access control with unique user identification; IP-ACL enforcement. TransformativIP Q-InfoSecur Module: Post-quantum encryption and decryption for ePHI access.**
Technical Safeguards	§164.312(b)	Audit controls: record and examine IS activity	**TransformativIP Core Modules + PQC Monitoring**	**TransformativIP Core Modules: Tamper-evident audit trail for every data exchange. PQC Monitoring: Network-level audit of all system activity including communications not logged by application-layer tools.**
Technical Safeguards	§164.312(c)	Integrity controls: protect ePHI from improper alteration or destruction	**TransformativIP Q-InfoSecur Module + TransformativIP Core Modules**	**TransformativIP Q-InfoSecur Module: Cryptographic integrity protection using ML-DSA digital signatures. TransformativIP Core Modules: IP-ACL prevents unauthorized modification of patient data at the cryptographic layer.**
Technical Safeguards	§164.312(d)	Person or entity authentication	**TransformativIP Core Modules + TransformativIP Q-InfoSecur Module**	**TransformativIP Core Modules: Identity management with multi-factor authentication. TransformativIP Q-InfoSecur Module: Hardware-bound quantum-resistant authentication that cannot be bypassed by session token theft.**
Technical Safeguards	§164.312(e)	Transmission security: encryption of ePHI in transit	**TransformativIP Q-InfoSecur Module**	**TransformativIP Q-InfoSecur Module: ML-KEM (FIPS 203) post-quantum key exchange and ML-DSA (FIPS 204) digital signatures for all ePHI transmissions. Exceeds current HIPAA encryption requirements and provides quantum resistance.**
Physical Safeguards (OT)	Not directly covered	Building systems affecting patient safety are NOT in HIPAA scope — this is the HIPAA blind spot	**PQC Monitoring**	**PQC Monitoring UNIQUELY addresses this gap: monitors building automation (HVAC, medical gas, power, elevators, fire safety) that HIPAA does not cover but patients' lives depend on.**

3. 21st Century Cures Act & TEFCA

Requirement	Authority	Requirement	Platform	How Addressed
Information Blocking Prohibition	Cures Act §171.103	Healthcare providers may not unreasonably restrict access to, exchange of, or use of EHI. Penalties up to 25% reduction in total Medicare revenue.	**TransformativIP Core Modules**	**TransformativIP Core Modules: Enables compliant data sharing while enforcing patient consent — prevents information blocking while maintaining privacy controls. FHIR R4 interoperability ensures data is accessible in required formats.**
Patient Access	Cures Act §171.301	Patients must be able to access their own EHI through standard APIs (FHIR)	**TransformativIP Core Modules**	**TransformativIP Core Modules: Full FHIR R4 server with patient-facing APIs; SMART on FHIR application launches; patient-controlled consent dashboard for granular data access management.**
TEFCA Participation	TEFCA Common Agreement	Participation in Trusted Exchange Framework through Qualified Health Information Networks (QHINs) for nationwide interoperability	**TransformativIP Core Modules**	**TransformativIP Core Modules: Direct QHIN connectivity through SMARTConnectivity module providing access to 99%+ of US providers. Consent enforcement maintained across all TEFCA exchanges.**
QHIN Security Requirements	TEFCA Security Framework	QHINs and participants must meet security requirements including encryption, access control, and audit logging	**TransformativIP Core Modules + TransformativIP Q-InfoSecur Module + PQC Monitoring**	**All three platforms: TransformativIP Core Modules provides access control and audit; TransformativIP Q-InfoSecur Module provides encryption exceeding TEFCA minimums; PQC Monitoring provides continuous security monitoring of QHIN connectivity infrastructure.**
API Condition of Certification	ONC Cures Act Final Rule	Health IT developers must publish APIs using FHIR standards; no special effort required from providers	**TransformativIP Core Modules**	**TransformativIP Core Modules: Certified FHIR R4 APIs; automatic translation between HL7 v2, FHIR, C-CDA, and X12 formats; no rip-and-replace of existing systems.**

4. Sensitive Data Categories & 42 CFR Part 2

Data Category	Regulatory Authority	Consent Requirement	Platform	How Addressed
United States Core Data for Interoperability (USCDI)	ONC USCDI v4+	Standard data elements required for interoperability; must be available through certified APIs	**TransformativIP Core Modules**	**TransformativIP Core Modules: Full USCDI support through FHIR R4 APIs with granular patient consent enforcement for each data element category via SMARTCompliance.**
Substance Use Disorder	42 CFR Part 2 (revised 2024)	Specific consent requirements for SUD treatment records; more restrictive than HIPAA; patient must consent to each disclosure; re-disclosure	**TransformativIP Core Modules**	**TransformativIP Core Modules: SMARTCompliance module implements 42 CFR Part 2 consent requirements at the data layer through IP-ACL. Consent decisions are cryptographically enforced — SUD data physically cannot be shared without patient authorization.**

		prohibited without consent		
Behavioral & Mental Health	State-specific laws (varies by state); HIPAA psychotherapy notes	Many states impose stricter consent requirements for mental health records than HIPAA baseline	**TransformativIP Core Modules**	**TransformativIP Core Modules: SMARTCompliance manages state-specific behavioral health consent requirements; IP-ACL enforces per-state rules at the data layer.**
Reproductive & Sexual Health	State-specific laws; Dobbs-related legislation	Highly variable by state; some states restrict interstate sharing of reproductive health data	**TransformativIP Core Modules**	**TransformativIP Core Modules: SMARTCompliance manages reproductive health consent with state-specific rules; IP-ACL prevents unauthorized interstate data sharing.**
Infectious Diseases / HIV/AIDS	State HIV/AIDS confidentiality laws; Ryan White Act	Most states require separate, specific written consent for HIV/AIDS test results and treatment records	**TransformativIP Core Modules**	**TransformativIP Core Modules: SMARTCompliance implements HIV-specific consent requirements; separate authorization workflow for HIV/AIDS data distinct from general medical records.**
Genetic Information	GINA (Genetic Information Nondiscrimination Act); state genetic privacy laws	Genetic information may not be used for insurance or employment decisions; separate consent often required for genetic data sharing	**TransformativIP Core Modules**	**TransformativIP Core Modules: SMARTCompliance manages genetic data consent separately from clinical records; IP-ACL prevents unauthorized genetic data disclosure to insurers or employers.**
Violence & Abuse Records	State mandatory reporting laws; VAWA; child abuse reporting statutes	Complex intersection of mandatory reporting obligations and victim privacy protections	**TransformativIP Core Modules**	**TransformativIP Core Modules: SMARTCompliance balances mandatory reporting requirements with victim privacy protections; manages consent exceptions for required disclosures.**
Social Determinants of Health (SDOH)	CMS SDOH screening requirements; state Medicaid programs	Sensitive non-clinical data (housing, food insecurity, transportation) requires careful consent management	**TransformativIP Core Modules**	**TransformativIP Core Modules: SMARTCompliance manages SDOH data consent; prevents non-clinical social data from being shared outside the care coordination context without patient authorization.**

5. FDA Medical Device Cybersecurity (Section 524B)

Requirement	FDA Guidance	Obligation	Platform	How Addressed
Premarket Cybersecurity Plan	FDA June 2025 Final Guidance	Manufacturers must submit cybersecurity plans as part of premarket submissions including threat modeling, security architecture, and	**TransformativIP Core Modules (data governance) + PQC Monitoring (network monitoring)**	**TransformativIP Core Modules: Consent framework for device-generated patient data. PQC Monitoring: Network monitoring environment data supports manufacturer's threat model validation.**

		vulnerability management		
Postmarket Cybersecurity Management	Section 524B lifecycle requirements	Manufacturers must monitor, identify, and address cybersecurity vulnerabilities throughout the device lifecycle	**PQC Monitoring**	**PQC Monitoring: Monitors the network environment where FDA-regulated devices operate; detects anomalous device behavior (unexpected communications, configuration changes, unauthorized associations) supporting postmarket surveillance.**
Software Bill of Materials (SBOM)	Section 524B SBOM requirement	Manufacturers must provide and maintain SBOMs for connected medical devices	**PQC Monitoring (validation)**	**PQC Monitoring: Passive device fingerprinting and version detection validates that deployed device firmware matches manufacturer SBOM declarations.**
Device Communication Security	FDA cybersecurity guidance	Connected devices must use authenticated and encrypted communications	**TransformativIP Q-InfoSecur Module**	**TransformativIP Q-InfoSecur Module: Post-quantum encryption for medical device communications; future-proofs device data against harvest-now-decrypt-later quantum threats.**
Healthcare Delivery Organization Obligations	Shared responsibility model	HDOs must maintain secure network environments for deployed medical devices	**PQC Monitoring**	**PQC Monitoring: Provides the continuous network monitoring that rural hospitals need to demonstrate they maintain a secure environment for connected medical devices.**

6. AI Governance & Consent

AI Use Case	Regulatory Concern	Consent Requirement	Platform	How Addressed
Clinical Decision Support	FDA regulation of AI/ML-based SaMD; state AI healthcare laws	Patient may need to consent to AI involvement in clinical decisions; varies by state	**TransformativIP Core Modules**	**TransformativIP Core Modules: Separate AI consent category for clinical decision support; patient can authorize or deny AI involvement independently from data sharing consent.**
Automated Decision-Making	State algorithmic discrimination laws; EU AI Act (for global orgs)	Patients must be informed when automated decisions affect their care; right to human review	**TransformativIP Core Modules**	**TransformativIP Core Modules: Separate consent category for automated decision-making; audit trail documenting AI involvement in care decisions.**
LLM Training Data	Emerging federal and state guidance; HIPAA de-identification requirements	Patient data used to train large language models requires explicit consent; de-identification may be insufficient	**TransformativIP Core Modules**	**TransformativIP Core Modules: Separate consent category for LLM training; IP-ACL physically prevents patient data from flowing to LLM training pipelines without explicit authorization.**
Third-Party AI Applications	Business associate agreements; state privacy laws	Third-party AI vendors accessing patient data must be authorized by patient and covered by BAA	**TransformativIP Core Modules**	**TransformativIP Core Modules: Separate consent category for third-party AI; IP-ACL enforces consent at the data layer for every third-party AI data exchange.**
Research AI	Common Rule (45 CFR 46); IRB oversight	Research use of patient data requires specific consent; IRB approval may be required	**TransformativIP Core Modules**	**TransformativIP Core Modules: Separate consent category for research AI; consent**

				enforcement distinct from clinical AI consent; supports IRB documentation requirements.
AI Agent Data Sharing & Monitoring	Emerging MCP (Model Context Protocol) standards; data governance frameworks	AI agents accessing and sharing patient data must be monitored, authenticated, and constrained by consent rules	**TransformativIP Core Modules (MCP Server) + PQC Monitoring**	**TransformativIP Core Modules: MCP server manages AI agent authentication, data access authorization, and consent enforcement for all agent interactions. PQC Monitoring: Monitors AI agent network behavior for anomalous data access patterns.**

7. Healthcare OT Security (Building Automation)

OT System	Patient Safety Impact	Protocol(s)	Platform	Detection Capability
HVAC & Environmental Control	OR temperature/humidity/pressure for surgical safety; ICU negative pressure for infection control; medication storage temperature	BACnet, Modbus, LonWorks, KNXnet/IP	**PQC Monitoring**	**PQC Monitoring: BACnet WriteProperty monitoring for setpoint changes; behavioral baselines for HVAC communication patterns; alert on unauthorized environmental control modifications.**
Medical Gas Distribution	Oxygen delivery for ventilator patients; surgical anesthesia gas mixtures; vacuum systems	BACnet, Modbus, proprietary	**PQC Monitoring**	**PQC Monitoring: Modbus register monitoring for medical gas alarm panels; zero-tolerance alerting on alarm threshold modifications; pressure anomaly detection.**
Electrical Power Distribution	Life-sustaining equipment requires continuous power; ATS must transfer within 10 seconds per NEC/NFPA	Modbus, BACnet, SNMP	**PQC Monitoring**	**PQC Monitoring: Power monitoring system configuration change detection; ATS controller behavioral baseline; generator start sequence verification.**
Pneumatic Tube Systems	Medication delivery (including time-critical chemotherapy); blood product transport; laboratory specimen transport	Proprietary (Swisslog, Pevco), BACnet	**PQC Monitoring**	**PQC Monitoring: Carrier routing anomaly detection; firmware vulnerability correlation (PwnedPiper class); communication pattern baselines for tube system controllers.**
Elevator & Vertical Transport	Patient transport between ED, OR, ICU; stretcher elevator priority systems	BACnet, Modbus, proprietary	**PQC Monitoring**	**PQC Monitoring: Elevator controller communication monitoring; priority override system access detection; service mode activation alerting.**
Fire & Life Safety	Fire alarm, sprinkler, smoke control, stairwell pressurization, nurse call systems	BACnet, Modbus, proprietary	**PQC Monitoring**	**PQC Monitoring: Fire panel communication monitoring; alarm suppression detection; nurse call system availability monitoring.**
Water Management	Legionella prevention; steam sterilization of surgical instruments	BACnet, Modbus	**PQC Monitoring**	**PQC Monitoring: Water treatment system monitoring; temperature control baseline; sterilization system availability tracking.**
Security & Access Control	Pharmacy controlled substance access; infant protection; behavioral health unit security	BACnet, OSDP, Wiegand	**PQC Monitoring**	**PQC Monitoring: Access control system communication monitoring; unauthorized access attempt detection; badge reader anomaly alerting.**

8. Proxy Authorization & Legal Relationships

Proxy Type	Data Access Scope	Legal Authority	Platform	How Managed
Power of Attorney	Agent may access medical records on behalf of incapacitated principal per scope of POA document	State POA statutes	**TransformativIP Core Modules**	**TransformativIP Core Modules: SMARTCompliance validates POA documentation; IP-ACL enforces access scope limitations per POA terms; audit trail documents all proxy access.**
Guardianship	Court-appointed guardian may access ward's medical records per court order scope	State guardianship / conservatorship laws	**TransformativIP Core Modules**	**TransformativIP Core Modules: SMARTCompliance manages guardianship credentials; validates court order scope; IP-ACL enforces access limitations.**
Attorney-Client	Attorneys may request medical records for litigation per signed authorization and applicable law	Attorney-client privilege; medical records request laws	**TransformativIP Core Modules**	**TransformativIP Core Modules: SMARTCompliance manages attorney authorization; validates signed releases; enforces scope limitations per authorization terms.**
Criminal Justice	Law enforcement may access records per valid court order or subpoena within defined scope	Court orders; subpoenas; state criminal justice information laws	**TransformativIP Core Modules**	**TransformativIP Core Modules: SMARTCompliance validates court orders/subpoenas; IP-ACL enforces access to only the records specified in the legal document.**
Educational Authorities	Schools may access student health records per FERPA exceptions and parental consent	FERPA; state education-health data sharing agreements	**TransformativIP Core Modules**	**TransformativIP Core Modules: SMARTCompliance manages FERPA-compliant educational access; validates parental consent; IP-ACL enforces school-specific access scope.**
Human Services	Social workers may access records per case assignment and statutory authority	State social services laws; child welfare statutes	**TransformativIP Core Modules**	**TransformativIP Core Modules: SMARTCompliance manages social services access credentials; validates case assignment; enforces statutory access scope.**
Housing & Shelter	Housing authorities may access health data for housing placement per consent and program requirements	HUD requirements; homeless services data sharing	**TransformativIP Core Modules**	**TransformativIP Core Modules: SMARTCompliance manages housing authority access; validates program enrollment; enforces consent-based data sharing.**
Military	Military health records may be shared between DoD, VA, and civilian providers per applicable agreements	DoD/VA health data sharing; TRICARE regulations	**TransformativIP Core Modules**	**TransformativIP Core Modules: SMARTCompliance manages military health data sharing agreements; validates service member authorization; IP-ACL enforces DoD/VA data handling requirements.**
Employment		ADA; FMLA; workers' compensation laws	**TransformativIP Core Modules**	**TransformativIP Core Modules: SMARTCompliance enforces strict scope limitations for employer access; validates signed authorizations; prevents disclosure beyond the minimum necessary standard.**

9. Platform Coverage Summary

Regulatory Domain	PQC Monitoring	TransformativIP Q-InfoSecur Module	TransformativIP Core Modules	Combined
CMS ATO (NIST 800-53)	CA-7, SI-4, CM, IR, RA, AC-4, AC-17, SC-7	IA-2, SC-8, SC-12, SC-13, SC-28	**AC-2, AC-3, AC-6, AU, IA, PL-2**	**COMPLETE COVERAGE of all ATO-required control families**
HIPAA Security Rule	Incident procedures, IS activity review, network monitoring, OT gap coverage	Encryption, integrity, authentication (all technical safeguards)	**Access control, audit controls, entity authentication, consent enforcement**	**COMPLETE COVERAGE including OT systems HIPAA does not address**
21st Century Cures Act / TEFCA	QHIN security monitoring	QHIN transmission encryption	**Information blocking prevention, patient access APIs, FHIR interoperability, QHIN connectivity**	**COMPLETE COVERAGE of Cures Act requirements**
42 CFR Part 2 & Sensitive Data (8 categories)	—	Encryption of sensitive data categories	**FULL COVERAGE of all 8 sensitive data categories through SMARTCompliance with IP-ACL enforcement**	**COMPLETE COVERAGE with cryptographic consent enforcement**
FDA Section 524B (Medical Devices)	Postmarket monitoring, network environment security, SBOM validation	Device communication encryption	**Device-generated data consent management**	**COMPLETE COVERAGE of both manufacturer and HDO obligations**
AI Governance (5 use cases + MCP)	AI agent behavioral monitoring	—	**FULL COVERAGE: 5 separate AI consent categories + MCP server for AI agent management**	**COMPLETE COVERAGE of AI consent + monitoring**
Healthcare OT / Building Automation	FULL COVERAGE: 8 building system categories, 340+ protocols, behavioral detection	—	**—**	**PQC Monitoring UNIQUE — no other platform or regulation addresses this**
Proxy Authorization (9 authority types)	—	—	**FULL COVERAGE: 9 proxy authority types with IP-ACL enforcement**	**TransformativIP CORE MODULES UNIQUE — no other platform manages this**
Post-Quantum Cryptography	Integrated TransformativIP Q-InfoSecur Module for platform encryption	FULL COVERAGE: FIPS 140-3 CVMP #4482, NIST FIPS 203/204/205, FDA ATO approved	**IP-ACL fused into PQC key structure**	**SHARED FOUNDATION across both platforms**
State-Specific Privacy/ AI Healthcare Laws	Network monitoring for compliance evidence	—	**SMARTCompliance manages 50-state regulatory variations**	**COMBINED COVERAGE of compliance enforcement + monitoring evidence**